This outline is provided as an EXAMPLE of a white paper to be submitted by vendors interested in obtaining certification and accreditation of a Digital Imaging (DI) System, Teleradiology (TR), or Picture Archiving Communications System (PACS). This outline is not all inclusive of the requirement, vendors must review all relevant references, DOD and Air Force Instructions, manuals and directives to meet the intent of this example outline and white paper format. Information provided will NOT be released to non-government agencies. The sole purpose of the data submission is for the government to determine a vendors ability to meet C2 and network security requirements.

Example

PACS and/or TR Vendor Security White Paper

Example

For assistance in obtaining electronic copies or additional references, Email your request to the Air Force Medical Logistics Office, Medical Technology Integration & Support Team POCs:

Michael Nielsen, Capt, USAF, MSC
Phone: 301-619-6872
Email: Michael.Nielsen@ft-detrick.af.mil

Steve Valentine, Contractor, Network Security Specialist
Phone: 301-619-6851
Email: Steve.Valentine@ft-detrick.af.mil

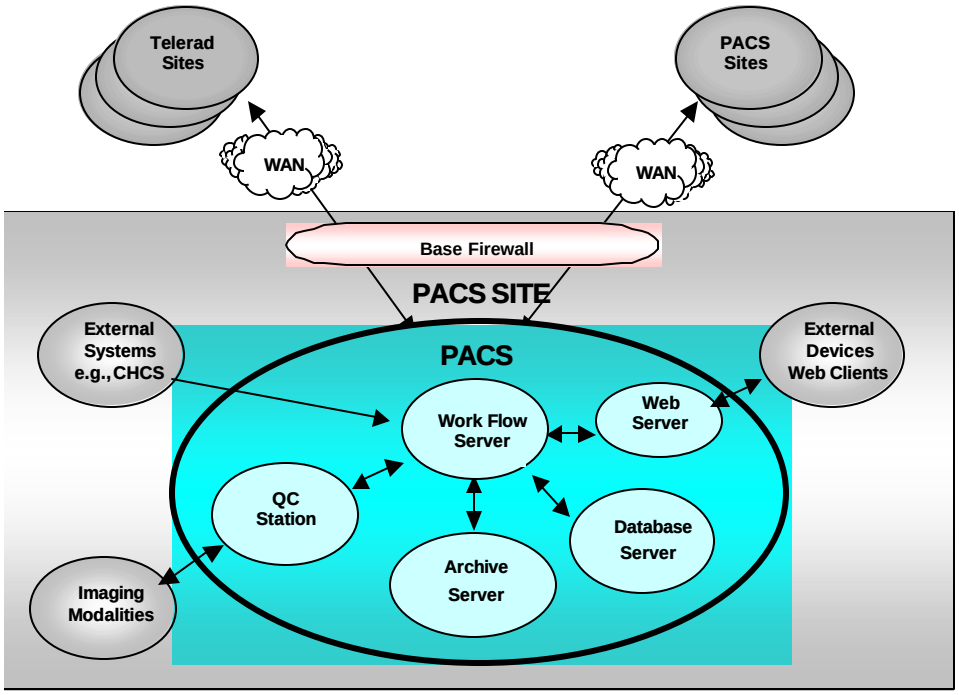
Forward

The scope of this plan is for a PACS or TR TCB inside any Medical Treatment Facility (MTF) for which a delivery order would be awarded. It also includes security measures for any communications connections to external networks including the Defense Information Systems Network (DISN), the internet (Web Clients), connections to other MTFs (which may be PACS/TR sites), dial-up connections to remote user locations. Based on the approaches described in the paragraphs below, security policies and procedures specific to each site will be provided prior to Site Acceptance Testing.

1. Introduction

Digital Imaging (DI) initiative is the term used to describe the Air Force Medical Service systems for acquiring, managing, interpreting, reviewing, and storing diagnostic images and related patient information. This document describes the security architecture of the Picture Archiving and Communications System (PACS) and/or the Teleradiology (TR) system implementation. PACS and TR are terms used for the remainder of this document to describe the generic turnkey or Commercial-Off-the-Shelf (COTS) solutions to be delivered to the Government under the DIN-PACS II contract.

PACS comprises a trusted computing base (TCB). The figure below illustrates a high-level view of the PACS subsystems (or TR subsystems) and their relationships to external systems.



A TCB is defined as …

2. System Architecture

2.1. PACS or TR Operational Concept

The following paragraphs describe a typical radiology workflow in terms of information flow within PACS/TR…

The patient arrives and demographics, exam information, and scheduling are entered into CHCS… a scenario for PACS or TR follows.

2.2. PACS or TR Modules

2.2.1. External Systems Interfaces

External systems are typically those that will remain in place and be connected to the PACS/TR system being installed. This includes Government Furnished Equipment (GFE), such as printers, modalities, desktop PC's and Network components.

2.2.1.1. Composite Health Care System (CHCS)

PACS or TR interface to CHCS will be unidirectional. PACS or TR accepts all CHCS data elements required to support the following functions:

2.2.1.2. Modalities

Modalities are the image acquisition devices within a given MTF. Modalities include:

PACS or TR communications with the modalities is governed by the Digital Imaging and Communications in Medicine (DICOM) version 3.0, (NEMA PS 3.1-9, 1993) Service Classes as explained below:

- Remote Verification.
- Modality Worklist.
- Storage Commitment.
- Query/Retrieve.
- Remote Storage

2.2.1.3. PACS Sites

The system interface between PACS or TR and PACS sites will be implemented via DICOM, TCP/IP, HL7, etc… Explain how you would do this and how you would meet security requirements in doing so.

2.2.1.4. MDIS Sites

The system interface between PACS or TR and MDIS sites will be implemented via DICOM, TCP/IP, HL7, etc… Explain how you would do this and how you would meet security requirements in doing so.

2.2.1.5. TR Sites

The system interface between PACS or TR and TR sites will be implemented via DICOM, TCP/IP, HL7, etc… Explain how you would do this and how you would meet security requirements in doing so.

2.2.2. Internal PACS or TR Modules

In the paragraphs below, describe the individual modules in terms of their functionality. (List and describe modules that are applicable to your PACS or TR system.) Include in the discussion where applicable to each module the following topics: Passwords, Logins, Remote Access, Filesystem Access, Applications, Logging and Auditing, Access Control, Network Management, User Management, Map Event Tables, Examples of Error Level Logging, Examples of Debug Level Logging, Remote Access Protection and File Protection. Include further discussion that would enable the government to gain a better understanding of how your system works and the security features you employ.

2.2.2.1. Workflow Servers

Include platform, operating system, configuration and workflow.

2.2.2.2. Quality Control Work Station

Include platform, operating system, configuration and workflow.

2.2.2.3. Web Server

Include platform, operating system, configuration and workflow.

2.2.2.4. Workstation Clients

Include platform, operating system, configuration and workflow.

2.2.2.5. Web Client Stations

Include platform, operating system, configuration and workflow.

2.2.2.6. RIS Gateway

Include platform, operating system, configuration and workflow.

2.2.2.7. RIS Server

Include platform, operating system, configuration and workflow.

2.2.2.8. RIS Workstation

Include platform, operating system, configuration and workflow.

2.2.2.9. RIS Reports Distribution Server

Include platform, operating system, configuration and workflow.

2.2.2.10. What ever is applicable ???

Include platform, operating system, configuration and workflow.

3. PACS or TR Block Diagram and Table of Information

3.1. PACS or TR Block Diagram

Provide a block diagram of your COTS PACS or TR product…

3.2. Table of Information for …Vendor Name… PACS or TR System

Item Name/COTS Name Hardware Description	Software Name/Release Number Version Number/Service Pack	Software Functional Description
Item Name: dBase Server HW:	Solaris, 8.0 ?	Operating System
		Database
		Login
		Calibration Application
		Display Support
		Library
		Cache Support
		client extensions
		dBase
		dB server extensions
		Service Tools
		WEB SERVICE
		Application Base Package
		Proxy Web Server
		Support package
		Dialup PPP
		Etc….

Item Name: Archive Server HW:	Solaris, 8.0 ?	Operating System
		Login
		Network Gateway
		MOD Jukebox archive
		Cache Support
		Client extensions
		dBase
		Service Tools
		Proxy Web Server
		Application Base Package
		Dialup PPP
		Support package
		Etc….
Item Name: Network Gateway HW:	Solaris, 8.0 ?	Operating System
		LOGINS
		Network Gateway
		MOD Jukebox archive
		Cache Support
		Client extensions
		DBase
		Service Tools
		Proxy Web Server
		Application Base Package
		Dialup PPP
		Support package
		Etc….
Item Name: QC Station HW: Intel Pentium IV, 1000 MHz	Microsoft NT Workstation 4.0, Service Pack xx	Operating System
	QC Station, version x.x.x	QC Station Software
	SCSI	CD-Writing Software
Item name: Web Server HW: Intel Pentium IV, 1500 MHz	Microsoft NT Server 4.0, Service Pack x	Operating System
	Microsoft SQL Server 7.0, Service Pack x	Database
	?	DICOM
	?	Java Runtime Environment
	128 bit	http Server
	Web 101	Application and Database Tables
Item Name: PACS Workstation HW: Intel Pentium IV, 1500 MHz	Microsoft NT Workstation 4.0, Service Pack x	Operating System
		PACS Workstation Application
	Client Applications	RIS Software
Item Name: Web Client Workstation HW: Government Furnished Equipment	Windows 2000, NT….	Operating System
	Netscape Navigator or Microsoft Internet Explorer (latest versions)	Web Browser
Item Name: RIS Gateway HW:	Microsoft NT Server 4.0, Service Pack x	Operating System
	Broker, v x , Service Pack x	HL7/DICOM gateway
	Microsoft SQL Server, v , Service Pack x	Database for RIS Gateway
	Report Interface, v xx	Web Server for retrieving reports
	Microsoft IIS	Microsoft Web Server
		Remote Software Maintenance
Item Name: RIS Server HW:	Open VMS 7.1	Operating System
	Server applications	Radiology Information System Application
	RDBMS v.	RDBMS
Item Name: RIS Workstation HW: Intel Pentium/IV PC	Microsoft NT 4.0, Service Pack xx	Operating System
	Client Applications	RIS Application
Item Name: RIS ?? Server HW: Intel Pentium/IV PC	Microsoft NT 4.0, Service Pack xx	Operating System
	Server Application	RIS ?? Server Application
Item Name: RIS ?? Server HW: Intel Pentium/IV PC	Microsoft NT 4.0, Service Pack xx	Operating System
	Server Application	RIS ?? Server Application

4. Network Security

This section addresses security considerations for both GFE, as well as vendor provided networks or network components. Specific MTF policies for firewall design, configuration, and implementation must be addressed in the network security architecture. This policy is needed to respond quickly and effectively to real or suspected breach or compromise of security system or policy. A thorough response policy will include analysis and policy development for the following:

- Intrusion and attack detection, identification and classification
- Attack containment, escalation procedures
- Assessing the full extent of attack and losses
- Assess the effectiveness of security strategies and policies
- Document the entire incident, providing recommendations for security architecture and policy improvement to prevent similar, future attacks
- Recovering from the attack.

5. Trusted Computing Base

It is a requirement that PACS or TR systems support C2 security, making users individually accountable through login procedures, auditing of security-relevant events, and resource isolation. In the following paragraphs describe the PACS or TR system attributes to meet or exceed minimal requirements for systems assigned a class (C2) rating.

This section of the document should be structured to follow the Orange Book requirements for a C2 level of trust. Each paragraph heading should correspond directly to a C2 requirement. Where applicable, the text body within each section may begin with the corresponding excerpt from the Orange Book. This is recommended for clarity, as well as, a road map for determination purposes.

5.1. Policy

The system security policy is a set of rules, and practices that regulate how the system manages, protects, and distributes sensitive information. Specifically, how are security events and policy violations (e.g., spoofing, denial of service attacks, unauthorized attempts to downgrade secure info, etc.) discovered. Explain how policies are enforced with regard to your PACS or TR system? Include the following subject areas in your discussion:

- Electronic Data Processing Security
- Communications Security
- Encryption of Sensitive Information and Data Circuits
- Personnel Security
- Physical Security

5.1.1. Discretionary Access Control

Orange Book Requirement:

"The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanis m (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals, or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users."

5.1.2. Object Re-use

Orange Book Requirement:

"All authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system."

5.2. Accountability

5.2.1. Identification and Authentication

Orange Book Requirement:

"The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual."

5.2.2. Audit

Orange Book Requirement:

"The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction or objects into a user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators and/or system security officers, and other security relevant events. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity."

5.3. Assurance

5.3.1. Operational Assurance

5.3.1.1. System Architecture

Orange Book Requirement:

"The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system. The TCB shall isolate the resources to be protected so that they are subject to the access control and auditing requirements."

5.3.1.2. System Integrity

Orange Book Requirement:

"Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB."

5.3.2. Life Cycle Assurance and Security Testing

Orange Book Requirement:

"The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB. Testing shall also include a search for obvious flaws that would allow violation of resource isolation, or that would permit unauthorized access to the audit or authentication data."

5.4. Documentation

5.4.1. Security Features User's Guide

Orange Book Requirement:

"A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another."

5.4.2. Trusted Facility Manual

Orange Book Requirement:

"A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given."

5.4.3. Test Documentation

Orange Book Requirement:

"The system developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and results of the security mechanisms' functional testing."

5.4.4. Design Documentation

Orange Book Requirement:

"Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. If the TCB is composed of distinct modules, the interfaces between these modules shall be described."

6. References

AFI 10-601, Mission Needs and Operational Requirements Guidance and Procedures, 13 Aug 99

AFI 10-602, Determining Logistics Support and Readiness Requirements, 20 Jun 94

AFI 14-111, Intelligence Support to the Air Force Acquisition Process, 1 Oct 97

AFI 14-201, Intelligence Production and Applications, 1 Feb 98

AFI 33-103, Requirements Development and Processing, 18 Mar 99

AFI 33-118, Radio Frequency Spectrum Management, 1 Aug 97

AFI 33-119, Electronic Mail (E-Mail) Management and Use, 1 Mar 99

AFI 33-129, Transmission of Information Via the Internet, 1 Aug 99

AFI 33-133, Joint Technical Architecture – Air Force, 1 Jul 00

AFI 33-136, Command, Control, Communications, Computers, and Intelligence Support Plans (C4ISP) and Certifications

AFI 33-201, (FOUO) Communications Security (COMSEC), 1 Aug 00

AFI 33-202, Computer Security, 15 Feb 01

AFI 33-321, Authentication of Air Force Records, 01 Apr 00

AFI 33-322, Records Management Program, 01 Dec 98

AFI 33-332, Air Force Privacy Act Program, 8 Nov 00

AFI 36-2201, Developing, Managing, and Conducting Training, 1 Apr 97, Change 1, 26 Apr 00

AFI 37-138, Records Disposition--Procedures and Responsibilities, 31 Mar 94

AFI 38-201 Determining Manpower Requirements, 1 Jan 99

AFI 63-101, Acquisition System, 11 May 94

AFI 63-1201, Assurance of Operational Safety, Suitability, and Effectiveness, 1 Feb 00

AFI 63-123, Evolutionary Acquisition for C2 Systems, 1 Apr 00

AFI 65-503, US Air Force Cost and Planning Factors, 4 Feb 94

AFI 99-101, Developmental Test and Evaluation, 1 Nov 96

AFI 99-102, Operational Test and Evaluation, 1 Jul 98

AFI 99-150, Combat Air Forces Test and Evaluation (in draft)

AFMAN 33-120, Radio Frequency (RF) Spectrum Management, 1 Jun 97

AFMAN 33-223, Identification and Authentication, 1 Jun 99

AFMAN 33-229, Controlled Access Protection (CAP), 1 Nov 97

AFMAN 37-123, Management of Records [to convert to AFMAN 33-323) 31 Aug 97

AFMAN 37-139, Records Disposition Schedule, 01 Mar 96

AFMAN 99-111, Command, Control, Communications, Computers and Intelligence (C4I) Test and Evaluation Process, 1 Mar 96

AFPD 33-2, Information Protection, 1 Dec 96

AFPD 99-1, Test and Evaluation Process, 22 Jul 93

AFSSI 5021, Time Compliance Network Order (TCNO) Management and Vulnerability and Incident Reporting, dated 1 Mar 2001

AFSSI 5027, (FOUO) Network Security Policy, 27 Feb 98

CJCSI 3170.01A, Requirements Generation System, 10 Aug 99

CJCSI 3312.01, Joint Military Intelligence Requirements Certification Process (DRAFT)

CJCSI 6212.01B, Interoperability and Supportability of National Security Systems, and Information Technology Systems, 8 May 00

CJCSI 6724.01 (Draft), C4I Systems Integration Management (SIM) Policy

DIA Regulation 55-3 Intelligence Support for Defense Acquisition Programs, 26 Jun 98

DIAM 57-1 General Intelligence Production, 24 Jan 97

DoD 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs, 1 Jan 01 [Interim]

DoD 5015.2-STD, Design Criteria Standard for Electronic Records Management Software Applications, Nov 97

DoD 5200.1-R, DoD Information Security Program, Jan 97

DoD 5200.28-STD, Trusted Computer System Evaluation Criteria, 26 December 1985

DoD 5200.2-R, Personnel Security Program, January 1987

DoD 5400.11-R, The Department of Defense Privacy Program, August 1983

DoD 5400.7-R, The Department of Defense Freedom of Information Act Program, September 1998

DoD 8510.1-M, Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) – Application Manual, July 31, 2000

DoD Architecture Framework 2.1 (Formerly C4ISR Architecture Framework 2.0)

DoDD 3222.3, Department of Defense Electromagnetic Compatibility Program (EMCP), 20 Aug 90

DoDD 4630.5, Compatibility, Interoperability, and Integration of Command, Control, Communications, and Intelligence (C3I) Systems, November 12, 1992

DoDD 4650.1, Management and Use of the Radio Frequency Spectrum, 24 Jan 87

DoDD 5000.1, The Defense Acquisition System, 23 Oct 00

DoDD 5015.2, DoD Records Management Program, 06 Mar 00

DoDD 5200.28, Security Requirements for Automated Information Systems (AISs), 30 Dec 97

DoDI 5000.2, Operation of the Defense Acquisition System, 23 Oct 00

DoDM 5000.4, Cost Analysis Guidance and Procedures, Dec 92

DoDM 8320.1-M, Data Administration Procedures, Mar 94

FIPS PUB 102, Guidelines for Computer Security C&A, Sep 83

National Security Directive 42 (1990)

OMB Circular A-11, Preparation and Submission of Budget Estimates, 1 Jul 98 [Revised Part I - 7 Nov 00]

OMB Circular A-130 (1985), Management of Federal Information Resources (1985), [Revised 28 Nov 00]

OSD Acquisition Deskbook C4I Support Plan Guidance and Format, 1 Dec 99

Public Law 100-235, Computer Security Act of 1987, 8 January 1988

Public Law 99-570, Freedom of Information Act of 1986

Secretary of the Air Force Order (No. 560.1), The Chief Information officer of the Air Force, 29 Oct 97